CERTIFICATE OF AUTHENTICITY OF DATA COPIED FROM AN ELECTRONIC DEVICE AND STORAGE MEDIUM PURUSANT TO FEDERAL RULE OF EVIDENCE 902(14)

I, William Paulemon, hereby declare and certify:

1. I am over 18 years of age, and I am currently employed by the Federal Bureau of Investigation as an Information Technology Specialist - Forensic Examiner (ITS-FE). I have been employed by the FBI for over 10 years.

2. As an ITS-FE with the FBI, I specialize in digital forensics, and I am responsible for conducting digital forensic examinations in support of criminal investigations. I have extensive training and experience in both making images of digital devices (*e.g.*, computer hard drives, external storage devices, thumb drives, and CDs/DVDs) extracting data from digital devices (*e.g.*, mobile phones), and examining and reporting relevant information found on such devices to criminal investigators and the U.S. Attorney's Office. In particular, I have attended trainings from Access Data, SANS, and FBI on imaging devices. I have conducted over 100 forensic examinations of digital devices in the course of my career, and I have made more than 100 images of, or extractions from, digital devices, including computers, external storage devices, and mobile phones.

3. In addition, I am proficient in the use of commercial forensic software, such as the software used during the course of this investigation: Tableau TD3 Forensic Imager.

4. I am qualified to authenticate the digital image referenced in this Paragraph because of my experience and training, and because I created the digital image listed below:

Original Device	Date of Image	Image Identifier
Hewlett-Packard hard drive (S/N: ST33000657SS)	08/16/2014	HQB000210

GOVERNMENT EXHIBIT 427

5. The device referenced above was imaged using specialized forensic tools and software. In my training and experience, forensic software and tools create accurate and reliable images of digital devices, and I have regularly relied on these tools to create accurate and reliable images of digital devices.

6. When imaging the device referenced in Paragraph 4, a "write blocker" was used, which is a piece of equipment or software that is especially designed to prevent the imaging process from changing or otherwise affecting any of the data on the device. Specifically, a Tableau TD3 Forensic Imager hardware write blocker was used to write block the device. Because write protection was used, I know that the original digital device was not altered during the imaging process.

7. When the initial image of the digital device listed in Paragraph 4 was created, a hash and a verification hash were obtained to confirm that the image was an exact duplicate of the original digital device. A hash is essentially a digital fingerprint of electronic evidence. If a single bit or character on a drive or other digital file is changed, the hash value of the entire drive will change. Because the hash of the original digital device and the hash of the image were identical, I know that the image I created was an exact duplicate of the original device.

8. Based on my training, experience, and my regular use of the tools and methods of imaging described above, I know that the imaging process created a true duplicate of the original device identified in Paragraph 4.

//

//

//

I declare, under penalty of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the foregoing information is true and correct. I further state that this certification is intended to satisfy Rule 902(14) of the Federal Rules of Evidence.

Executed this 10th day of November in 2020.

William Paulemon